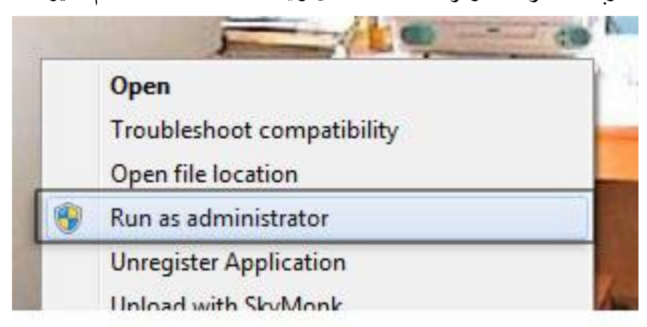
كيف تكتشف أن جهازك مخترق ؟

بشكل عام ان الحصول على برامج او ملفات او افلام من مواقع او اشخاص غير موثوق فهم هى اولى خطوات تسهيل الهاكر فى مهمته … ولكن الهاكر قد يحاول بطرق متعددة بجعلك تثق فيه لكى تفتح الرابط الذى يرسله لك او تفتح الاميل المرسل لك منه بعدة طرق واخرها فى السنوات الاخيرة بأن يرسل لك رسالة من اميل صديق لك .. وايضا قد يرسل لك صورة تظنها عادية وهى قد تحتوى على برنامج خبيث فبمجرد ان تحمل وتفتح الصورة يعمل البرنامج بدون ان تشعر..ولكن بصورة عملية وفى نقاط معدودة كيف تكتشف أن جهازك مخترق :-

١ - برامج او حسابات غريبة

احيانا قد تجد على جهازك برامج مثبتة لم تقم انت بتنزيلها .فلو وجدت على جهازك برنامج غريب لم تقم بتثبيته فقد يكون هذا أحد دلائل اختراق جهازك (ولكن ايضا لابد ان تضع فى اعتبارك انه قد يكون هذا البرنامج احد تحديثات الويندوز او تحديث لبرنامج اخر) . او عندما تجد account غريب فى المستخدمين لم تقم بإنشاؤه او لو وجدت ان الحساب الذى تستخدمه على الجهازقد تم تغيير الباسورد الخاص به او قد تجد ان حساب الزبون Guest المعطل دائما على الكمبيوتر قد تم عمل تفعيل له فهذا من الدلائل الواضحه ان جهازك تعرض للاختراق ، ولهذا ينصح دائما عدم استخدام حساب الادمن الرئيسى الAdministrator سواء فى المنزل او فى العمل ،فأنت بذلك سهلت على الهاكر نصف مهمته وهو تخمين اسم المستخدم ويتبقى له الباسورد وايضا يفضل عدم استخدام حساب ادمن باسم مختلف عن اسم الادمن الرئيسى فأنت بذلك نعم صعبت على الهاكر مهمته قليلا ولكن الهاكر لديهم ايضا برامج يستطيعون بها معرفه هل هذا الحساب ادمن ام لا والاصح ان تقوم باستخدام اكونت محدود الصلاحيات بحيث لو تعرض للاختراق فلن يكون لديه صلاحيات كاملة للتحكم فى جهازك او فى الشبكة و وعندما تريد استخدام اى برنامج بمميزات الادمن فهناك يمكن استخدام ميزة run as admin ، وبذلك تكون قد وفرت لنفسك الامان وايضا استطعت استخدام مميزات الادمن .



٢ - هاك الإميل

- قد تصحى من النوم وتجد اتصالا من احد اصدقائك يقول لك ايه الاميل اللى انت ارسلته لى امبارح ده ، ويقرأ لك الاميل فتقول له انا لم ارسل هذا الاميل ابدا ابدا ، ثم يعيد صديقك ارسال الاميل لك لتفحصه بنفسك وعندها تتأكد ان اميلك ارسل رسالة لصديقك هذا او لاصحابك كلهم بدون ان تدرى ، فعندها لا تحاول سب الاميل وتقول له "ايه اللى انت بتعمل ده يابن اللذينه " ، ولكن وضع فى اعتبارك ان جهازك قد يكون تم اختراقه بالفعل .
- نقطة بسيطة احب ان اضيفها فى هذا الجانب قد يحاول الهاكر بجعلك ارسال رساله له حتى لو فارغة وذلك لكى يتعرف على ال ip الخاص بجهازك او شبكتك و لوقمت بهذا فعندها اصغر هاكر يستطيع معرفة الايبى الخاص بك سواء من الاميل نفسه او عن طريق برنامج مساعد (وان شاء الله احاول شرح هذا فى تدوينات اخرى)

- الخلاصة ان لاتحاول فتح اميل لشخص لاتثق به وايضا لاتحاول ارسال رسالة بدون داعى سواء لشخص لاتثق به او لشخص تعرفه فقد تأتى بعض المشاكل من المقربون وانا لاادعوك بالشك فى الجميع ولكن عليك بالحذر.

٣ - حركات غريبة للكمبيوتر

- اذا وجدت جهازك يقوم بحركات غريبة مثل الماوس يتحرك لوحده او يقوم بكتابة اشياء على الجهاز فعندها قد يكون جهازك تحت السيطرة عن بعد ويقوم احد الاشخاص بالتحكم بجهازك ويرى كل شىء على جهازك كأنه جالس معك ، وهنا عليك بالحذر جدا عند استخدام برامج المحادثات والدردشة مثل الياهو السكاى بى وغيرها.
- اثناء تشغيل الويندوز وعند الدخول لسطح المكتب اذا وجدت شاشة سوداء تفتح وتقفل بسرعة فهذا قد يكون احد الدلائل ان تم تنزل احد البرامج على جهازك بدون موافقتك، ولكنه ليس دليل أكيد.
- اذا وجدت ان الصفحة الرئيسية للمتصفح الخاص بك قد تغيرت او تم تنزيل تولبار غريب فهذا قد يكون من الدلائل الواضحه ان جهازك تم اختراقه.
- اذا وجدت ان برنامج الحماية الخاص بك او الفايروول قد تم تعطيلة او تم ازالته فهذا دليل أكيد ان جهازك تعرض للاختراق.

٤ - بطء الكمبيوتر او الشبكة

عندما تجد ان جهازك بطىء جدا مع انك لم تفتح إلا صفحة ويب واحدة وانت متأكد انه بحالة سليمة جدا ، او تجد ان شبكة العمل الخاص بك بطيئة جدا فى وقت غير الطبيعى ويستهلك ترافيك عالى جدا فعندها يكون عليك استخدام احد البرامج لقياس ومراقبة ترافيك الشبكة او استخدام الهاردوير فايرول الخاص بك لمراقبة هذا الترافيك لمعرفة من أين تأتى المشكلة ،فقد يكون احد الموظفين هو المتسبب فى هذا باستخدام خاطىء للانترنت او باستخدامه لبعض البرامج التى تستخدم بروتوكول UDP ، او قد يكون احد الهاكر يتحكم فى جهازك او الشبكة عن بعد وبالتأكيد هذا يؤدى لبطء الشبكة .

٥ - سجلات تسجيل الأحداث LOG

لو كان لديك على جهازك برنامج جدار نارى او كان لديك فى الشبكة الخاصه بك روتر فهنا يمكنك استخدام اللوج او سجلات تسجيل الاحداث ويطلق عليها فى الويندوز ايضا event viewer، فى مراقبة من حاول الدخول على جهازك او الشبكة بطريقة غير مصرح بها ، ولكن ايضا لابد ان تضع فى اعتبارك ان الهاكر المحترفين لهم القدرة على تغيير هذا السجلات لتجعلك تقرأ اشياء غير صحيحة .

٦ - برامج وطرق اكتشاف الاختراق

- يعتبر استخدام البرامج او الاوامر من الطرق المفضلة عند الكثيرين لمعرفة هل الجهاز او الشبكة تم اختراقه ام لا ومنها على سبيل المثال port scanner فهو يقوم بفحص البورتات والمنافذ لديك وايضا يمكنك عمل هذا عن طريق امر netstat عن طريق شاشة cmd السوداء فهذا الامر ترى به المنافذ المفتوحة و الاتصال المفتوح مع الاخرين على الانترنت وعليك هنا ان تقارن بما انت تعمل عليه فعليا على الجهاز من مواقع انترنت وبما تراه على الشاشة السوداء

  والذى يظهر ليس اسم الموقع ولكن ايبهات وعليك هناك انت تقوم بعمل بنج على الموقع لو انت فاتح ياهو مثلا اعمل بنج على موقع ياهو وقارن بعد ذلك الايبهات هل مماثلة ام لا.
- ادخل على run ثم اكتب msconfig ثم ادخل تحت تاب startup وهنا تجد البرامج التى تعمل عند فتح الويندوز ، فاذا وجدت برنامج غريب لم تقم بتنزيله او لا تعرفه فاحذف الاشارة من علامة المربع بجوار البرنامج ، (ولكن عليك

الحذر من حذف اى برنامج قديكون اساسى فى عمل الويندوز فهذا قد يؤدى لمشاكل فى الجهاز ومع ذلك ستجد ان بجوار اسم كل برنامج مساره الخاص يساعدك فى معرفه ماهيه البرنامج).

- من البرامج المساعدة هو برنامج Hijack this فهو برنامج يساعدك فى رؤية ماهى البرامج المثبته على جهازك كلها ويمكنك بعد ذلك من حذف البرامج الضارة .

٧ - برامج عدوه الفايروول

هناك برامج لاتستطيع ان تعمل مع وجود جدار نارى على الكمبيوتر مثل برامج P2P وهنا فأنت تكون بلاشك عرضه للاختراق بسهوله.

واخيرا لو كنت تريد ان تعمل على جهاز أمن ١٠٠% فأنصحك ان تغلق الكمبيوتر وتضع فى الصندق الخاص به ، فليس هناك جهاز أمن تماما ولكن هناك طرق تصعب على المخترق الوصول لمعلومات .

و احب ان اعرف رأيكم في هذا التدوينة لكى استمر فى هذه الموضوعات عن

كيف تكتشف ان جهازك مخترق كيف تحمى جهازك وماهى اهم البرامج الاختراق وماهى اساليب وطرق الاختراق وفى حالة اختراق الجهاز ماذا افعل ؟

<u>من المصادر التى تمت الاستعانة بها</u>

www.computerhope.com

www.ehow.com

www.internetgeeks.org

م.محمد عز الدين عبدون

https://www.facebook.com/computer.networks

http://comprnetworks.wordpress.com